ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Laboratorio di
Sicurezza Informatica

Esercitazione: Host Intrusion Detection Systems

Andrea Melis
Marco Prandini
Dipartimento di Informatica – Scienza e Ingegneria

Agenda

- Cenni/Definizioni HIDS
  - Definizione
  - HIDS vs NIDS
  - Tecniche
- AIDE
- Wazuh

HIDS

- Come discusso in precedenza, un sistema di rilevamento delle intrusioni è un'applicazione hardware o software che rileva e avvisa gli amministratori quando viene rilevata un'attività dannosa.

- HIDS si concentra principalmente sul monitoraggio e l'analisi dei file di registro al fine di rilevare anomalie e alterazioni non autorizzate sulla base di politiche predefinite e una serie di regole.

HIDS

- In altre parole, l'HIDS è efficace quanto le regole prestabilite che si sono configurate.
- Con un gran numero di registri archiviati, l'estrazione di informazioni significative è fondamentale per rilevare le anomalie.
- Le informazioni estratte dovrebbero essere sempre il più possible accurate.
- Pertanto, garantire la sicurezza di tali registri è essenziale.

Anomaly Based vs. Signature Based IDS

- Anomaly based
  - Monitora il traffico di rete
  - Tiene traccia dei modelli di traffico e delle informazioni per ottenere dati di riferimento
  - Se viene rilevata una deviazione nel comportamento della rete, l'IDS rileverà un attacco.
  - Elevato rischio di falsi positivi
- Signature based
  - Il database delle firme degli attacchi viene mantenuto localment
  - Confronta il traffico con il database
  - Se viene trovata una corrispondenza, viene inviato un avviso
  - Richiede aggiornamenti costanti

HIDS vs NIDS

- NIDS
  - Monitora tutto il traffico sulla rete
  - Utile per monitorare sistemi non critici.
- HIDS
  - IDS personalizzato per un server specifico
  - Essere più vicini all'host consente maggiori possibilità di rilevamento
  - Impedisce l'installazione all'interno della rete di minacce quali Trojan e backdoor

AIDE

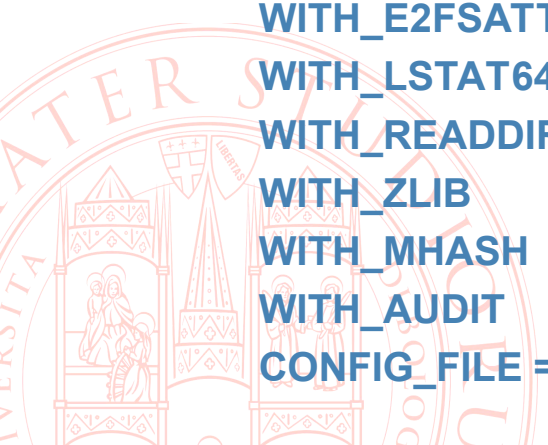
- AIDE è un sistema di rilevamento delle intrusioni che rileva le modifiche ai file sul sistema locale.
  - Crea un database dalle regole delle espressioni regolari che trova dal file di configurazione.
  - Una volta inizializzato, questo database può essere utilizzato per verificare l'integrità dei file.
  - Supporta diversi algoritmi di hashing del messaggio (md5, sha1, rmd160, tiger, haval, ecc.) utilizzati per verificare l'integrità del file.
  - È possibile aggiungere più algoritmi con relativa facilità.
  - È possibile specificare diverse proprietà e attributi per il monitoraggio.
  - Alcune delle proprietà dei file che AIDE può controllare sono:
    - Permessi
    - inode
    - Timestamp modifica
    - Contenuto
    - Utente
    - Gruppo
    - Dimensione del file
    - ...

Configurare AIDE

- Puoi controllare la versione installata e le opzioni con cui AIDE è compilato eseguendo il comando

```
aide -v
```

```
Aide 0.16.1
Compilato con le seguenti opzioni:
WITH_MMAP
WITH_PCRE
WITH_POSIX_ACL
WITH_SELINUX
WITH_XATTR
WITH_E2FSATTRS
WITH_LSTAT64
WITH_READDIR64
WITH_ZLIB
WITH_MHASH
WITH_AUDIT
CONFIG_FILE = "/dev/null"
```



Installare AIDE

- Installare aide sulla macchina Kali del laboratorio con:

  sudo apt install aide

  (o in alternativa senza sudo ma da shell di root)

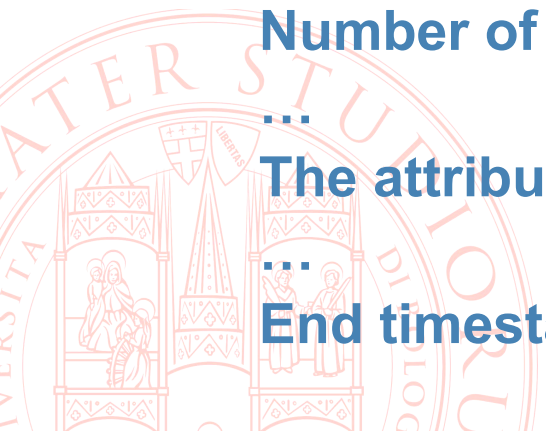
Configurare AIDE

- Il file di configurazione generale per AIDE si trova in:
  - /etc/default/aide.
- Le regole e le configurazioni risiedono in:
  - /etc/aide/
- Il database AIDE si trova in:
  - /var/lib/aide/

Configurare AIDE

- Prima di procedere con la configurazione specifica su AIDE è necessario prima di tutto creare un nuovo database AIDE.
- Per fare questo è sufficente usare il comando aideinit, che crearà un nuovo databse in:
  - /var/lib/aide/aide.db.new
- Lanciare quindi da root:

```
aideinit
...
AIDE initialized database at /var/lib/aide/aide.db.new
...
Number of entries: XXXXXX
...
The attributes of the (uncompressed) database(s):
...
End timestamp: DATE TIME +0300 (run time: 6m 53s)
```



Configurare AIDE

- È stato quindi creato il nuovo database, andiamo quindi a metterlo nel path corretto.

  `cp /var/lib/aide/aide.db{.new,}`

- Per riaggiornare la configurazione di AIDE presente in

  /etc/aide/aide.conf

- È sufficente lanciare il comando

  `update-aide.conf`

- Il comando genera un nuovo file di configurazione in

  /var/lib/aide/aide.conf.autogenerated

- È possibile quindi copiare il nuovo file di configurazione su quello di default:

  `cp /var/lib/aide/aide.conf.autogenerated /etc/aide/aide.conf`

Test con AIDE

- A questo punto abbiamo una prima versione di AIDE configurata, possiamo quindi lanciare una prima verifica di consistenza tra il database e i file monitorati col comando:

  aide -c /etc/aide/aide.conf -C

  questo comando impiega un po di tempo a completare
  il risultato è la verifca delle modifiche nel filesystem sotto tag come:

  Added entries:

  ...

  Oppure

  Changed entries:

Test con AIDE

- Vediamo però come aide si accorga dei cambiamenti introdotti manuale.

- Andiamo quindi a creare dei file sulla cartella /etc con:

```
echo "1.2.3.4 labsectest.com" >> /etc/hosts

touch /etc/nuovofile

rm -rf /etc/issue
```

Test con AIDE

- Dopo aver fatto i precedenti cambiamente lanciamo nuovamente il comando di verifica.
- Possiamo sempre lanciare quello completo con:

  aide -c /etc/aide/aide.conf -C

- Ma è possibile limitare a runtime il check specificando soltanto la sottocartella da monitorare con:

  aide -c /etc/aide/aide.conf --limit /etc --check

  dovreste vedere quindi i cambiamenti come:
  Added entries:
  f++++++++++++ /etc/nuovofile
  Removed entries:
  f---------------- /etc/issues
  ecc

Test con AIDE

- Invece che specificare a mano il range di monitor è possibile decidere direttamente quali cartelle includere e quali escludere dal file di configurazione
- Alla fine del file aide.conf aggiungere con la seguente notazione per escludere delle cartelle:

  !/home/

  !/var/lib/

  !/proc

- O specificarne una senza il “!” per restringere il range da monitorare.

Test con AIDE: Configurazione Custom

- Proviamo ora a creare un nostra configurazione personalizzata di AIDE.

- Creiamo quindi una cartella e inseriamo il file di configurazione assegnato a lezione:

```
mkdir /home/kali/aide

cp aide.conf /home/kali/aide/aide.conf
```

Test con AIDE: Configurazione Custom

- Analizziamo quindi la configurazione data:

```
# Databases Path
database=file:/home/kali/aide/aide.db
database_out=file:/home/kali/aide/aide.db.new
database_new=file:/home/kali/aide/aide.db.new

# Set your own AIDE rule

SecLabRule=p+n+u+g+s+m+c+xattrs+md5+sha512

# Direc/files to monitor with rules
....
# Dir to ignore
/home/kali SecLabRule
!/root
```

Test con AIDE: Configurazione Custom

- Abbiamo creato un nuovo database, impostato un monitoring sulla cartella /home/kali secondo la nostra regola e un ignore sulla cartella di root

  SecLabRule=p+n+u+g+m+c+xattrs+md5+sha512

- La seguente regola controlla quindi cambiamenti:

  p = permission

  n = number of links

  u = user

  g = group

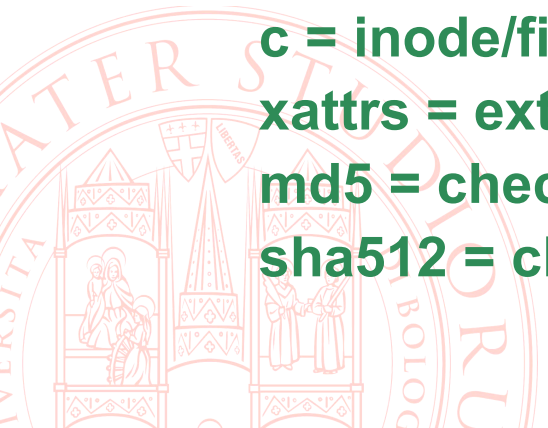
  m = modification time

  c = inode/file change time

  xattrs = extended file attributes

  md5 = checksum

  sha512 = checksum



Test con AIDE: Configurazione Custom

- A questo punto reinizializziamo il il database con la nuova configurazione

```
aide -c /home/kali/aide/aide.conf -i
```

- Copiamo il database

```
cp /home/kali/aide/aide.db{.new,}
```

- Verifichiamo la correttezza della configurazione

```
aide -c /home/kali/aide/aide.conf --config-check
echo $?
```

deve restituire 0

Test con AIDE: Configurazione Custom

- A questo punto facciamo delle modifiche, sia nella cartella /home/kali sia su quella di root

```
touch /root/testroot
touch /home/kali/testsec
mkdir /home/kali/testsecfold
rm /home/kali/aide/aide.db.new
```

- Lanciamo quindi AIDE con il nostro file di conf e vediamo i cambiamenti registrati

```
aide -c /home/kali/aide/aide.conf -C
```

Altre configurazioni implementabili

- Invio su mail. L'output dei checks viene spedito all'utente specificato in MAILTO = del file di configurazione /etc/default/aide. Di defaul è settato root ma è possibile specificare un indirizzo mail dopo aver configurato MTA

```
#MAILTO=root
```

- Aggiungere aide come task in cronjob per fare un check ogni 10 minuti

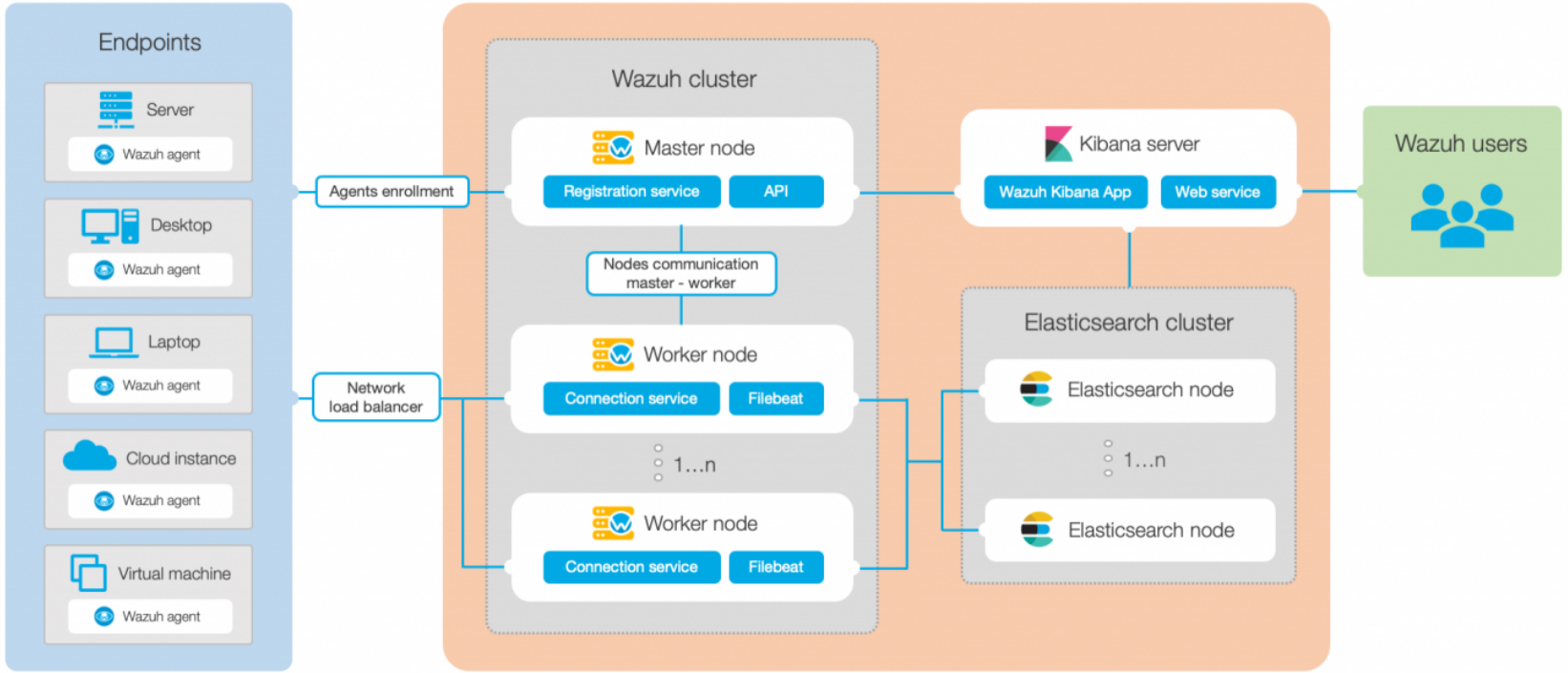
```
sudo crontab -e

*/10 * * * * aide -c /home/kali/aide/aide.conf -u && cp
/home/kali/aide/aide.db{.new,}
```

Wazuh

- Wazuh è un HIDS open-source, molto usato in ambito aziendale.
- È altamente customizzabile e permette di gestire le intrusioni nella propria rete di device attraverso la modalità manager over agents.
- Ha diverse funzionalità tra le quali:
  - Vulnerability Tests
  - Integrity Tests
  - Log-based Intrusion Detection
  - Active Response
  - Ecc
- Per maggiori informazioni la documentazione di Wazuh è disponibile su: https://documentation.wazuh.com/current/index.html

Wazuh Architettura



- Manager
  - Clusters
  - Kibana
  - Elasticsearch
- Agents
  - Device da monitorare

Wazuh esercitazione

- Scopo dell'esercitazione è capire il funzionamento di Wazuh in linea molto generale, e fare il test sul rilevamento di un attacco

- Compito dello studente sarà quindi:

  - Scaricare e importare la VM di Wazuh-Manager
  - Installare l'agent di Wazuh sulla macchina del laboratorio registralo come agent attivo sul Wazuh Manager.
  - Registrare l'agent sul Wazuh Manager.
  - Creare un'active response local e server di un attacco a scelta.

  I dettagli dell'esercitazione e i comandi li trovate su virtuale.unibo.it